UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF ALABAMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH CELL PHONE ACCOUNT [redacted] THAT IS STORED AT PREMISES CONTROLLED BY **T-MOBILE, USA INC**.	**FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Randall Hoffman, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by T-Mobile, USA Inc. ("T-Mobile"), a wireless provider headquartered in New Jersey. The information to be searched and seized is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 2703(c)(1)(A) to require T-Mobile to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications, related to the account associated with cellular telephone number [redacted] (hereinafter the "**Subject Cellular Telephone**"). The information to be seized is described in the following paragraphs and in Attachment A and Attachment B.

2. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

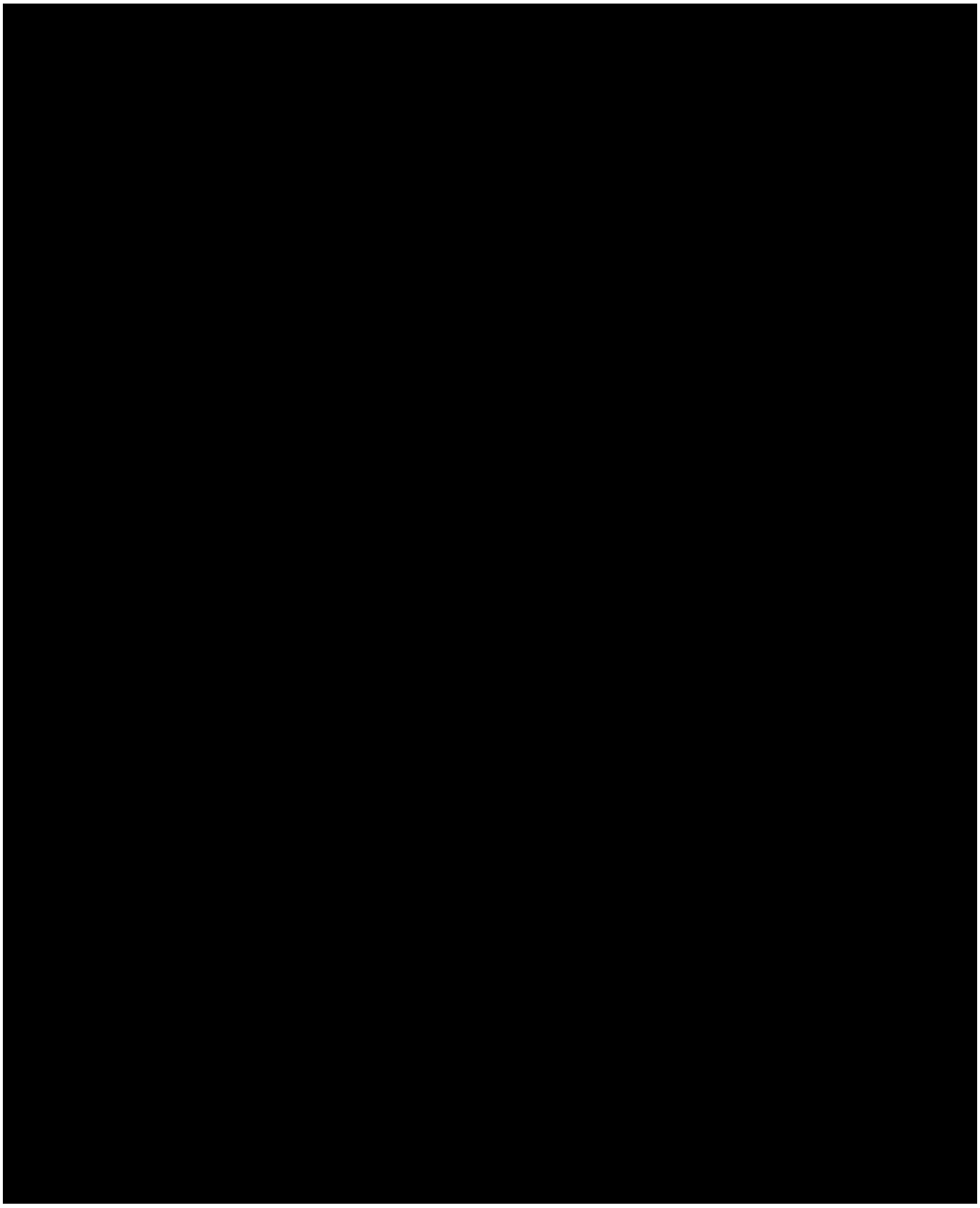
3. I, Randall L. Hoffman, being duly sworn, depose and state:

I am a Special Agent with Homeland Security Investigations (HSI). I am presently assigned to the Office of the Resident Special Agent in Charge in Mobile, Alabama (RAC Mobile). I have been so employed with HSI since November 2001. As part of my daily duties as an HSI Special Agent, I investigate criminal violations relating to the national security of the United States such as drug smuggling, arms trafficking, and financial crimes, including money laundering and bulk cash smuggling. I am authorized by the Homeland Security Act of 2002 to perform the duties provided by law and regulation, and empowered to conduct investigations of offenses against the United States; conduct searches without warrant at the border or its functional equivalent; conduct inquiries related to alienage and removability; execute and serve search and arrest warrants; serve subpoenas and summonses; administer oaths; make arrests without warrant; require and receive information relating to offenses; and bear firearms.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and others involved in the investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. All dates, times, locations, and amounts are approximations.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 841 (Possession with Intent to Distribute Cocaine) have been committed by [redacted] and [redacted] in the Southern District of Alabama and elsewhere. There is also probable cause to search the information for evidence of these crimes, as described in Attachment A.

[redacted]



Case 1:23-mj-00135-MJ-WS-B Document 7-1 Filed 06/15/23 Page 5 of 13 PageID #: 22

[redacted]

14. Based on training and experience, your affiant believes that historic cellular telephone records for the **Subject Cellular Telephone** would enable Law Enforcement to confirm the identity of the person utilizing that phone number and determine that individual's location at the time that the messages in question were sent.

15. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public.

16. Wireless phone providers typically generate and retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

17. Many wireless phone providers generate and retain information about the location in which a particular communication was transmitted or received. Your affiant is aware, through training and experience, that when a cellular device is used to make or receive a call, or text message, or other communication, the wireless phone provider will maintain a record of which cell tower was used to process that contact. In general, but not always, the cellular telephone at issue will use the closest unobstructed tower that generates the strongest signal. These wireless providers maintain this information, including the corresponding cell towers (i.e., antenna towers covering specific geographic areas), "sectors" (i.e., faces of the towers), and other signaling data, as part of their regularly conducted business activities. Typically, a wireless provider maintains a record of the cell tower information associated with calls. These cell tower records are sometimes referred to as "cell site" data.

18. Because the cellular device generally attempts to communicate with the closest unobstructed tower, by reviewing the above-described information, your affiant and other law enforcement officers can determine the approximate geographic area from which the communication originated or was received.

19. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

20. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service used, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the

dates and times of payments and the means and source of payment (including any credit card or bank account number).

21. Wireless Providers also retain the content of communications for a limited period of time. Obtaining the content of messages sent to and receive from the number listed in Attachment A will aid in determining if a federal crime was committed, as outlined above.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

22. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. § 2703(c)(1)(A), by using the warrant to require Sprint to disclose to the government copies of the records and other information (excluding the content of communications) particularly described in Section I of Attachment A. Upon receipt of the information described in Section I of Attachment A, government-authorized persons will review that information to locate the items described in Section II of Attachment A.

23. Because the information is to be provided by T-Mobile and does not involve any physical intrusion by the government or any investigative agency, it is respectfully suggested that the normal time constraints requiring that the warrant be executed only in the daytime are not applicable.

CONCLUSION

24. Based on the foregoing, I submit that there is probable cause to conclude that that the cellular telephone having the number [redacted] was possessed by [redacted] and/or [redacted] while committing violation of 21 U.S.C. § 841 and was used to facilitate and coordinate that violation and that the requested information associated with the cellular telephone as further described herein and in Attachment A, is available from T-Mobile and that information,

including cell site information, constitutes evidence of violations of 21 U.S.C. § 841 Accordingly, I respectfully request that the Court issue the proposed search warrant.

Respectfully submitted,

RANDALL L HOFFMAN
Digitally signed by RANDALL L HOFFMAN
Date: 2023.06.13 11:47:57 -05'00'

RANDALL L. HOFFMAN
Special Agent
Department of Homeland Security
Homeland Security Investigations (HSI)

THE ABOVE AGENT HAD ATTESTED TO THIS AFFIDAVIT PURSUANT TO FED. R. CRIM. P. 4.1(b)(2)(A) THIS _____, JUNE 15, 2023.

P. Bradley Murray
Digitally signed by P. Bradley Murray
Date: 2023.06.15 10:03:33 -05'00'

HONORABLE P. BRADLEY MURRAY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

1. The cellular telephone assigned call number [redacted] (the "Account") whose wireless service provider is T-Mobile USA, Inc. a company headquartered in New Jersey.
2. Records and information associated with the Target Cell Phone that is within the possession, custody, or control of T-Mobile USA, Inc. including information about the historical location of the cellular telephone and contents of communications, as further described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by T-Mobile

T-Mobile, USA Inc. is required to disclose the following records and other information, if available, to the United States for the cellular telephone having the number [redacted] which are stored at premises owned, maintained, controlled, or operated by T-Mobile, a wireless provider located in New Jersey ("Account"), for the time period May 1, 2023 to the present:

A. The following information about the customers or subscribers of the Account:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions; to include IP data session reports with associated cell site information;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
9. The content of communications, to the extent that they are available or were preserved.

B. All records and other information (including the contents of communications) relating to the Account, including:

1. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

2. All data about which "cell towers" (i.e., antenna towers covering specific geographic areas), "sectors" (i.e., faces of the towers), and (if available) "azimuth" received a radio signal from each cellular telephone or device assigned to the Account; and

3. RTT records, PCMD records, NELOS records, Timing Advance records, TrueCall records, MDT GPS records, and all other records containing timing advance measurements and distance-to-tower measurements for all technologies (CDMA, GSM, UMTS, LTE, etc.); and

4. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 21 U.S.C. § 841 (Possession with Intent to Distribute Cocaine) involving the user of the account since May 1, 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) The location of the user of the account at times relevant to the investigation.

(b) The content of user or owner's communications that may be evidence of the alleged crime;

(c) The content of communications concerning the account user or owner's efforts to conceal the crime;

(d) The identity of the person(s) who created or used the account or identifier, including records that help reveal the whereabouts of such person(s).

(e) The identity of witnesses and/or co-conspirators with whom the account user communicated.